IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCHES OF: 6811 Jefferson Davis Highway, Trailer 98 North Chesterfield, VA 23237; THE PERSON OF AMBROCIA MARTINEZ; AND THE PERSON OF CARLOS ORELLANA.	Case No. 3:23-sw- 25 Case No. 3:23-sw- 26 Case No. 3:23-sw- 27 **FILED UNDER SEAL**

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A A WARRANT TO SEARCH AND SEIZE

I, Wessam E. Faltas, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with Homeland Security Investigations ("HSI") within Immigration and Customs Enforcement ("ICE"), Department of Homeland Security ("DHS"), and have been so employed since March 2019. As a Special Agent with HSI, I am authorized to investigate crimes involving violations of federal law, including violations of Title 18 of the United States Code, Section 2252A, involving child exploitation and child pornography offenses. Prior to becoming an HSI Special Agent, I served as a Criminal Investigator with the Department of Defense Pentagon Force Protection Agency from April 2017 to March 2019. I also served as an ICE Deportation Officer in Buffalo, New York and Richmond, Virginia from December 2008 to April 2017 and as a United States Customs and Border Protection Officer in Buffalo, New York from July 2002 to December 2008.

2. I am a graduate of the Federal Law Enforcement Training Center ("FLETC") in Glynco, Georgia. At FLETC, I was trained in, among other things, criminal investigative

techniques and child exploitation investigations. I am empowered by law to investigate and make arrests for violations of federal law, including child exploitation and child pornography offenses, and to execute warrants issued under the authority of the United States.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other sworn law enforcement officers. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

4. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search: (1) the premises known as **6811 Jefferson Davis Highway, Trailer 98, North Chesterfield, VA 23237** ("**SUBJECT PREMISES**"), located within the Eastern District of Virginia and further described in Attachment A-1, for the things described in Attachment B; (2) the person of **AMBROCIA MARTINEZ ("SUBJECT PERSON 1")**, and the person of **CARLOS ORELLANA ("SUBJECT PERSON 2")**, further described in Attachments A-2 and A-3, respectively, for the things described in Attachment B. Attachments A-1, A-2, A-3, and B are incorporated by reference.

5. I have probable cause to believe that the SUBJECT PREMISES contains contraband, evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A (certain activities relating to material constituting or containing child pornography). I submit this application and affidavit in support of a warrant to search the SUBJECT PREMISES and seize evidence, fruits, and instrumentalities of the foregoing crimes. I request authority to search the entire SUBJECT PREMISES, including the residential dwelling and any computers, smartphones, communication devices, and electronic media located therein, where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as contraband,

instrumentalities, fruits, and evidence of crime. I also request authority to search SUBJECT PERSON 1 and SUBJECT PERSON 2, as described respectively in Attachments A-2 and A-3, for any computers, smartphones, mobile communication devices, and electronic media, and to seize all items listed in Attachment B as contraband, instrumentalities, fruits, and evidence of crime.

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C § 2711. Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated," and "is in . . . a district in which the provider . . . is located or in which the wire or electronic communications, records, or other information are stored." 18 U.S.C. §§ 2711(3)(A)(i)-(ii).

LEGAL AUTHORITY

7. 18 U.S.C. § 2252A prohibits a person from knowingly transporting, shipping, receiving, attempting to receive, distributing, reproducing for distribution, or possessing any child pornography, as defined in 18 U.S.C. § 2256(8), when such child pornography was either mailed, shipped or transported using any means of facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, by any means including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce.

DEFINITIONS

8. Based on my training and experience, I use the following terms to convey the following meanings:

a. **Child Erotica:** materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. **Child Pornography:** any visual depiction of sexually explicit conduct where (a)

the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

c. **Visual depictions:** undeveloped film and videotape, data stored on computer disk or by electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. *See* 18 U.S.C. § 2256(5).

d. **Sexually explicit conduct:** actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, oral-anal, or anal-genital, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person. *See* 18 U.S.C. § 2256(2).

e. **Minor:** any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

TECHNICAL TERMS

9. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. GPS: A GPS navigation device uses the Global Positioning System ("GPS") to display its current location. It often contains and records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations

involved in such navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

b. **Wireless telephone**: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include GPS technology for determining the location of the device.

c. **Digital camera**: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic films. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

d. **Portable media player**: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

e. **Computer**: As defined pursuant to 18 U.S.C. § 1030(e)(1) a computer is "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions and including any data storage facility or communications facility directly related to or operating in conjunction with such device."

f. **Computer server**: A computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the internet. A domain name system ("DNS") server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol ("IP") address so the computer hosting the web site may be located, and the DNS server provides this function.

g. **Computer hardware**: Consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but are not limited to, central processing units, internal and peripheral storage devices, such as fixed disks, internal hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but are not limited to, keyboards, printers, video display monitors, and related communication devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but are not limited to, physical keys and locks).

h. **Computer software**: Digital information which can be interpreted by a computer or any of its related components to direct the way they work. Computer software

is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications and utilities.

i. **PDA**: A personal digital assistant ("PDA") is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work word-processing documents, spreadsheets, and presentations. PDAs may also include GPS technology for determining the location of the device.

j. **Tablet**: A tablet is a mobile computer that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called applications or "apps," which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit access to the Web, sending and receiving e-mail, and participating in Internet social networks.

k. **Internet**: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international

borders, even when the devices communicating with each other are in the same state.

l. **Internet Service Providers ("ISPs")**: Commercial organizations that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and location of computers and other communication equipment. ISPs can offer a range of options in providing access to the Internet, including telephone-based dial-up, broadband based access via digital subscriber line ("DSL") or cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based on the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a username or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

m. **Internet Protocol address ("IP address"):** A unique numeric address used by a computer on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most ISPs control a range of IP addresses. Some computers have static, that is

long-term IP addresses, while other computers have dynamic, or frequently changed IP address.

n. **Records, documents and materials:** All information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, and paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, and typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

o. **Website:** Textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language ("HTML") and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol ("HTTP").

p. **Storage medium:** Any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, external hard drives, and other magnetic or optical media.

q. **Log Files:** Records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide

range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

r. **Peer-to-peer (P2P):** P2P file sharing is a method of communication available to Internet users through the use of special software or applications. The software is designed to allow users to trade digital files through a network that is formed by linking computers together. A significant distinction between P2P networks and traditional computer networks is that P2P machines generally communicate directly with each other, rather than through a relatively low number of centrally based servers. Because of the decentralized nature of P2P networks, they are commonly used by collectors and traders of child pornography.

a. **Smartphone:** A portable personal computer with a mobile operating system having features useful for mobile or handheld use. Smartphones, which are typically pocket-sized (as opposed to tablets, which are larger in measurement), have become commonplace in modern society in developed nations. While the functionality of smartphones may vary somewhat from model to model, they typically possess most if not all of the following features and capabilities: 1) place and receive voice and video calls; 2) create, send and receive text messages; 3) voice-activated digital assistants (such as Siri, Google Assistant, Alexa, Cortana, or Bixby) designed to enhance the user experience; 4) event calendars; 5) contact lists; 6) media players;

7) video games; 8) GPS navigation; 9) digital camera and digital video camera; and 10) third-party software components commonly referred to as "apps." Smartphones can access the Internet through cellular as well as Wi-Fi ("wireless fidelity") networks. They typically have a color display with a graphical user interface that covers most of the front surface of the phone and which usually functions as a touchscreen and sometimes additionally as a touch-enabled keyboard.

b. **SIM card:** SIM card stands for a "subscriber identity module" or "subscriber identification module," which is the name for an integrated circuit used in mobile phones that is designed to securely store the phone's international mobile subscriber identity ("IMSI") number and its related key, which are used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers). It is also possible to store contact information on many SIM cards.

CHARACTERISTICS OF COLLECTORS OF CHILD PORNOGRAPHY

10. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereinafter, "collectors").

11. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.

12. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, drawings, and/or

other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature, and sexual aids.

13. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.

14. Collectors almost always possess and maintain their "hard copies" of child pornographic images and reference materials (*e.g.,* mailing and address lists) in a private and secure location. With the growth of the internet and computers, many collections are maintained in digital format. Typically, these materials are kept at the collector's residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and the legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods, even for years. Collectors often discard child pornography images only while "culling" their collections to improve their overall quality.

15. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.

16. Collectors prefer not to be without their child pornography for any prolonged periods of time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

17. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation between subscription and collection behavior has been repeatedly confirmed during nationwide law enforcement initiatives.

18. In sum, collectors of child pornography frequently maintain their collections in a private and secure location such as their residence, often in digital format, for long periods of time. They also maintain information related to their receipt or distribution of such media in that location, including correspondence with and contact information for other individuals distributing or sharing child pornography.

USE OF PEER-TO-PEER AND BITTORRENT

19. This investigation involves a user of "BitTorrent," which is an internet-based P2P network that allows users to anonymously receive and share files, chat on message boards, and access websites within the network.

20. P2P file-sharing is a method of communication available to internet users using special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. These P2P networks are commonly referred to as decentralized networks because each user of the network can distribute information and queries directly through other users of the network, rather than relying on a central server to act as an indexing agent, where all the information is first deposited before it is distributed. A user first obtains the P2P software, which can be downloaded from the Internet.

In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. However, only files that are specifically stored in shared folders are exchanged. Therefore, a user needs simply to move a file from one folder to another to stop the distribution across the Internet. Further, once a file or files are placed in a shared folder, its distribution is dependent only on the machine being turned on and connected to the Internet.

21. BitTorrent is a type of P2P file sharing software. Users of the BitTorrent network wishing to share new content will use a BitTorrent program to create a "torrent" file for the file or group of files they wish to share. A torrent file is a small file that provides a method for a user to download the file(s) referenced in the torrent from other BitTorrent users. Torrent files are typically found by using keyword searches on Internet sites that host or link to them. Torrent files may be referenced by their "infohash," which uniquely identifies the torrent based on the file(s) associated with the torrent file. To download a file(s) from other users on the BitTorrent network, a user typically obtains a torrent file. The BitTorrent software processes the information in the torrent file and locates devices on the BitTorrent network sharing all or parts of the actual file(s) being sought. The download of the content referenced in the torrent is achieved after the requesting computer and the sharing computer(s) directly connect to each other through the Internet using the BitTorrent software.

22. One of the advantages of P2P file sharing is that multiple files may be downloaded at the same time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a BitTorrent user downloading a movie file may actually receive parts of the movie from multiple computers. The advantage of this is that it speeds up the time it takes to download the file. It is possible to also download the file or files from only one computer.

Law enforcement software downloads files and/or parts of files from a single computer or device at a single IP address.

23. The BitTorrent Network bases all of its file shares on the Secure Hash Algorithm 1 ("SHA1"). This mathematical algorithm allows for the digital fingerprinting of data. Once you check a file or files with a SHA1 hashing utility capable of generating this SHA1 value (the fingerprint), a fixed-length unique identifier is assigned to that file. The SHA1 hash is the current Federal Information Processing and Digital Signature Algorithm. The SHA1 is secure because it is computationally infeasible for two files with different content to have the same SHA1 hash value.

24. A P2P file transfer is assisted by reference to an IP address. This address, expressed as four groups of numbers separated by decimal points, is unique to a particular computer during an online session. The IP address provides a unique location making it possible for data to be transmitted between computers.

PROBABLE CAUSE

25. Homeland Security Investigations in Richmond, VA ("HSI Richmond") utilizes a software program to identify individuals who use peer-to-peer networks to exchange child pornography. A device using IP address **173.53.5.34** ("**TARGET IP**") was running BitTorrent and advertised that it contains files available to download, meaning that the user utilized a device with that TARGET IP to store files in shared folders, thus making them exchangeable. HSI Richmond used law enforcement software to download Child Sexual Abuse Material ("CSAM") from a device that is using the TARGET IP. The law enforcement software identified the IP address of the source computer or device as the TARGET IP.

26. On October 25, 2022, HSI Richmond downloaded a media file from a BitTorrent user at the TARGET IP containing 4 image files of nude prepubescent girls, approximately 9 to 11

years old, engaging in sexually explicit conduct with nude adult males. 2 of the 4 image files were composite images, containing 16 photos each, that appeared to be screen captures made from a single video. One of the 2 composite images was complete and the second was incomplete, with 4 of the 16 screen-captures in the composite image being partially visible, and with the remainder being fully visible.

27. On November 06, 2022, HSI Richmond downloaded a second media file from a BitTorrent user at the TARGET IP. The file contains 145 photos, of which approximately 125 depict prepubescent girls engaging in sexually explicit conduct with other children and with nude adults. 8 of the image files were complete composite images containing multiple photos that appeared to be screen captures made from a single video. The media file also contained 2 complete videos; the first is of a prepubescent girl, approximately 11 years old, engaging in sexually explicit conduct with a nude adult male. This video was about 8 minutes long and showed acts that included oral and vaginal penetration. The second video is about 4 minutes long and shows a nude prepubescent girl, approximately 12 years old, manipulating her vaginal area with a foreign object.

28. On November 15, 2022, your affiant requested subscriber information from Verizon for the TARGET IP. Verizon provided the following information to HSI Richmond:

Name	Maria Martinez
Address	6811 Jefferson Davis Highway, Lot 98, Richmond, VA 23237
Email	Ambrocia_m@yahoo.com
Phone Number	(804) 301-3214 and (804) 275-6175
Username	Maria.martinez93

29. On November 18, 2022, your affiant requested subscriber information from T-Mobile for phone number (804) 301-3214, the first phone number associated with the TARGET IP. T-Mobile provided the following information to HSI Richmond:

Name	Carlos A. Orellana
Address	6811 Jefferson Davis Highway, Trailer 98, North Chesterfield, VA 23237

30. On November 18, 2022, your affiant requested subscriber information from Verizon Wireless for phone number (804) 275-6175, the second phone number associated with the TARGET IP. Verizon Wireless provided the following information to HSI Richmond:

Name	Maria Martinez
Address	6811 Jefferson Davis Highway, Trailer 98, North Chesterfield, VA 23237

31. On November 18, 2022, your affiant requested subscriber information from Yahoo (Oath Holdings Inc.) for the email address ambrocia_m@yahoo.com, the email address associated with the TARGET IP. Yahoo provided the following information to HSI Richmond:

Name	Ambrocia Martinez
Zip/Postal Code	23237
Recovery Email:	orellanacarli@gmail.com
Recovery Phone:	(804) 412-5646

32. On January 26, 2023, your affiant requested subscriber and billing information from Google, Inc. for the email address orellanacarli@gmail.com, the above referenced recovery email address. Google, Inc provided the following information to HSI Richmond:

Name	Carlos Orellana
Billing Address	6811 Jefferson Davis Highway, Lot 98, Richmond, VA 23237
Recovery Email	ambrocia_m@yahoo.com
Phone Number	(804) 412-5646
Payment Information	Visa card ending in 7250 Carlos Orellana Richmond, VA 23237

33. On December 9, 2022, your affiant requested subscriber information from T-Mobile Wireless for phone number (804) 412-5646, the phone number associated with both ambrocia_m@yahoo.com and orellanacarli@gmail.com. T-Mobile Wireless provided the following information to HSI Richmond:

Name	Carlos A Orellana
Address	6811 Jefferson Davis Highway, Trailer 98, North Chesterfield, VA 23237

34. HSI Richmond conducted surveillance of the SUBJECT PREMISES on several occasions in November and December 2022. On November 22, 2022, and December 20, 2022, HSI Richmond observed a blue Hyundai Elantra bearing Virginia plate number UGF6942 (SUBJECT VEHICLE) parked at the SUBJECT PREMISES. Virginia Department of Motor

Vehicles ("VADMV") records revealed the vehicle is registered Carlos Alberto Orellana at the SUBJECT PREMISES.

35. VADMV lists the SUBJECT PREMISES as the current address on Carlos Orellana's and Ambrocia Martinez's Driver's License files. Ambrocia Martinez is Carlos Orellana's mother.

36. Ambrocia Martinez was previously encountered by U.S. Border Patrol in El Paso, TX and used the name Maria Ambrosia Castro-Marquez. Martinez has also used the aliases Maria Ambrocia Martinez, Maria Ambrosia Marquez, Ambrosia Marquez Martinez, Maria Martinez, and Maria Ambrosia Castro.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

37. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES or on the SUBJECT PERSON(s), in whatever form they are found. One form in which the records might be found is digital data stored on a computer's hard drive or other storage media, or on a smartphone's internal memory or SIM card. Thus, the warrant applied for would authorize the seizure of electronic storage media (including smartphones) or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

38. *Probable cause.* I submit that if a computer or storage medium is found on the SUBJECT PREMISES or on the SUBJECT PERSON(s), there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost.

Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Depending on a variety of factors, a particular computer could easily not overwrite deleted files with new data for many months, and in certain cases conceivably ever.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

39. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes

described in the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

e. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

f. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who

used or controlled the computer or storage medium at a relevant time.

g. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

h. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

i. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

j. I know that when an individual uses a computer to possess, receive, distribute and/or produce child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also

likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

40. *Necessity of seizing or copying entire computers, smartphone, or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

k. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can

take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

l. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the SUBJECT PREMISES. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

m. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

41. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

42. *Biometrics.* Based on my training and experience, I know that many computers, mobile phones and other mobile electronic devices offer their users the ability to unlock the device

via the use of a fingerprint or thumbprint (collectively, a "fingerprint") in lieu of a numeric or alphanumeric passcode or password. Each device's manufacturer may have a specific name for this feature, but collectively, this feature will be called fingerprint unlock.

43. If a user enables fingerprint unlocking on a given device, they can register one or multiple fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's fingerprint sensor.

44. Some devices are not equipped with fingerprint sensors, or the user has not enabled the feature that allows for the use of a fingerprint to unlock the device. A device may have a feature that allows its user to utilize facial, iris or retina recognition software, to unlock the device. These features require the user to place their face in front of the device's camera(s), with both eyes open, for a sufficient period to unlock the device.

45. In certain circumstances, a fingerprint or facial recognition cannot be used to unlock a device that has one or both those features enabled, and a passcode or password must be used instead. These circumstances typically include when more than a predetermined period of time has passed since the last time the device was unlocked. Thus, in the event law enforcement encounters a locked device, the opportunity to unlock the device via fingerprint, facial-, iris-, or retina-recognition unlocking may exist only for a short time. Fingerprint, facial-, iris-, or retina-recognition unlocking may also not work to unlock the device if: (1) the device has been turned off and restarted; (2) the device has received a remote lock command; and/or (3) multiple unsuccessful attempts to unlock the device via fingerprint unlocking are made.

46. The passcodes or passwords to the devices in the SUBJECT PREMISES and/or on the SUBJECT PERSON(s) are not known to law enforcement. Thus, it will be likely be necessary

to press the SUBJECT PERSON(s)' fingerprint(s)s into the fingerprint sensor(s) or use facial-, iris- or retina-recognition software of one or more devices. Attempting to unlock the relevant device(s) via fingerprint, facial-, iris- or retina-recognition software is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

47. For the reasons described above, this affiant requests that the Court authorize law enforcement to press the fingers (including thumbs) of the SUBJECT PERSON(s) to the touch ID sensor(s) of devices found in the SUBJECT PREMISES or on the SUBJECT PERSON(s) to unlock the devices to search for the contents as authorized by this warrant. In the event the device(s) is locked with facial-, iris- or retina-recognition software, this affiant requests the Court authorize law enforcement to use the devices' cameras to capture the image of the user to unlock the device.

48. Because several people share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well. If it is determined that any of the devices seized are the property of a third party, and no incriminating material is found on those devices, those devices will be returned to their rightful owner as soon as practicable.

CONCLUSION

Based on the foregoing, I submit that there is probable cause to believe that: (1) an individual or individuals at the SUBJECT PREMISES used a computer, mobile device, or other electronic device connected to the internet from the SUBJECT PREMISES to violate Title 18,

United States Code § 2252A; and (2) the fruits, evidence, contraband, and instrumentalities of these offenses, described in Attachment B, are presently located at the SUBJECT PREMISES and/or on the SUBJECT PERSON(s). Permission is expressly sought to seize any mobile devices, computer hardware, storage media, computer software, and computer-related documentation located at the SUBJECT PREMISES or on the SUBJECT PERSON(s) and subsequently conduct an on-site and off-site forensic examination, as necessary, using whatever data analysis techniques needed to seize the contraband, evidence, and instrumentalities listed in Attachment B. This includes the use of biometrics to unlock one or more of the devices on the SUBJECT PERSON(s) and in the SUBJECT PREMISES.

I respectfully request, therefore, that the Court issue the attached warrant authorizing the searches of the SUBJECT PREMISES and the SUBJECT PERSON(s) (described in Attachments A-1, A-2, and A3) and seizure of the items listed in Attachment B.

WESSAM E FALTAS Digitally signed by WESSAM E FALTAS Date: 2023.02.07 13:38:56 -05'00'

Wessam Faltas
Special Agent
Homeland Security Investigations

Sworn and attested to me by the affiant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone this 8th day of February, 2023

/s/ MRC
MARK R. COLOMBELL
UNITED STATES MAGISTRATE JUDGE

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF: 6811 Jefferson Davis Highway, Trailer 98 North Chesterfield, VA 23237	Case No. _____ **FILED UNDER SEAL**

ATTACHMENT A-1

DESCRIPTION OF PREMISES TO BE SEARCHED

The premises to be searched is known as 6811 Jefferson Davis Highway, Trailer 98, North Chesterfield, VA 23237. The premises are located in the Shady Hill Mobile Home Community and are described as a one-story mobile home with a mix of green and tan vinyl siding and green trim around the roof. The structure has a set of stairs leading to the main entry and the number "98" is displayed in red on the right side of the main entrance. The front door is white and has a six-panel glass window. There is one window on the front of the mobile home to the left of the front door.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF: THE PERSON OF AMBROCIA MARTINEZ	Case No. _____ **FILED UNDER SEAL**

ATTACHMENT A-2

DESCRIPTION OF PREMISES TO BE SEARCHED

Law enforcement may search the persons of the following individuals:

Ambrocia Marquez MARTINEZ
Date of Birth: 02/18/1965; 03/31/1966; 02/18/1963; 03/08/1965
Aliases: Maria Ambrocia MARTINEZ; Maria Ambrosia CASTRO Marquez; Maria Ambrosia MARQUEZ; Ambrosia MARQUEZ Martinez; Maria Ambrosia CASTRO; Maria MARTINEZ
Race: White, Hispanic
Sex: Female
Address: 6811 Jefferson Davis Highway, Trailer 98
North Chesterfield, VA 23237
Weight: 180 lbs
Height: 5'05"
Eyes: Brown
Hair: Black
SSN: ***-**-3916 and ***-**-8275

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF: THE PERSON OF CARLOS ORELLANA	Case No. _____ **FILED UNDER SEAL**

ATTACHMENT A-3

DESCRIPTION OF PREMISES TO BE SEARCHED

Law enforcement may search the persons of the following individuals:

Carlos Alberto ORELLANA
Date of Birth: 06/20/1996
Race: White, Hispanic
Sex: Male
Address: 6811 Jefferson Davis Highway, Trailer 98
North Chesterfield, VA 23237
Weight: 200 lbs
Height: 5'07"
Eyes: Brown
Hair: Black
SSN: ***-**-9244

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCHES OF: 6811 Jefferson Davis Highway, Trailer 98 North Chesterfield, VA 23237; and THE PERSON OF AMBROCIA MARTINEZ; and THE PERSON OF CARLOS ORELLANA.	Case No. 3:23-sw- Case No. 3:23-sw- Case No. 3:23-sw- **FILED UNDER SEAL**

ATTACHMENT B

PROPERTY TO BE SEIZED

1. All fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 2252A relating to the distribution, receipt and possession of child pornography, including:
   a. Any and all visual depictions of minors;
   b. Any and all address books, names and lists of names and addresses of minors;
   c. Any and all diaries, notebooks, notes, and other records reflecting physical contacts, whether real or imagined, with minors;
   d. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids;
   e. Records and information relating to the BitTorrent network and/or P2P programs;
   f. Records and information relating to Internet Protocol (IP) address **173.53.5.34**, such as billing statements, written correspondences and any other documents showing the subscriber information for the internet service(s) at the SUBJECT PREMISES.
2. Computers, smartphone, or storage media used as a means to commit the violations described above.
3. Any computer, smartphone, or storage media whose seizure is otherwise authorized by this

warrant, and any computer, smartphone, or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER").

a. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondences;

b. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. Evidence of the lack of such malicious software;

d. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER.

f. Evidence of the times the COMPUTER was used;

g. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. Records of or information about Internet Protocol addresses used by the COMPUTER;

j. Records of, or information about, the COMPUTER's Internet activity, including

firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

k. Contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

5. During the search, law enforcement officials may photograph the searched SUBJECT PREMISES to record the condition thereof and/or the location of items therein.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer, smartphone, or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

As to mobile devices, smartphones, and/or tablets recovered during the execution of this search warrant, law enforcement is permitted to: (1) depress Ambrocia Martinez's and/or Carlos Orellana's thumbs and/or fingers onto the fingerprint sensor of the device (only when the device

has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of Ambrocia Martinez's and/or Carlos Orellana's face with the person's eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in *Graham v. Connor*, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts.

If the government identifies seized materials, that are potentially attorney-client privileged or subject to the work product doctrine ("protected materials"), the Prosecution Team will discontinue review until a Filter Team of government attorneys and agents is established. The Filter Team will have no previous or future involvement in the investigation of this matter. The Filter Team will review all seized communications and segregate potentially protected materials, i.e. communications to/from an attorney, or that otherwise reference or reflect attorney advice. At no time will the Filter Team advise the Prosecution Team of the substance of any of the potentially protected materials. The Filter Team then will provide all communications that are not potentially protected materials to the Prosecution Team and the Prosecution Team may resume its review. If the Filter Team decides that any of the potentially protected materials are not protected (e.g., the

communication includes a third party or the crime-fraud exception applies), the Filter Team must obtain either agreement from defense counsel/counsel for the privilege holder or a court order before providing these potentially protected materials to the Prosecution Team.